UM

AO 91 (Rev. 11/11) Criminal Complaint

AUSA John Kness (312) 469-6042

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

FILED

MAR - 4 2016
3-4-16
THOMAS G. BRUTON
CLERK, U.S. DISTRICT COURT

UNITED STATES OF AMERICA

v.

JOHN REYNALD SOLERO and
YURI VENTANILLA

CASE NUMBER:
UNDER SEAL

16CR 147

CRIMINAL COMPLAINT MAGISTRATE JUDGE FINNEGAN

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

From in or around October 2013 to in or around August 2015, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendants violated:

Code Section	*Offense Description*
Title 18, United States Code, Sections 1030(b) and 1030(a)(4)	Defendants conspired with each other and with others known and unknown, knowingly and with intent to defraud, to access a protected computer, without authorization, thereby furthering the intended fraud and obtaining a thing of value, namely, goods and services belonging to Company A and its clients, including travel and electronic merchandise.

This criminal complaint is based upon these facts:

X Continued on the attached sheet.

ROBERT MEININGER
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: March 4, 2016

Judge's signature

City and state: Chicago, Illinois

SHEILA FINNEGAN, U.S. Magistrate Judge
Printed name and Title

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS | ss

AFFIDAVIT

I, ROBERT MEININGER, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation, and have been so employed for over four years. My current responsibilities include the investigation of criminal violations relating to computer access, in violation of 18 U.S.C. §§ 1030 and 1343. I am assigned to a cybercrime squad at the FBI and have gained experience in the investigation of computer crimes during this time.

2. This affidavit is submitted in support of a criminal complaint alleging that John Reynald SOLERO and Yuri VENTANILLA have violated Title 18, United States Code, Sections 1030(b) and 1040(a)(4) (the "Subject Offenses"). Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint charging SOLERO and VENTANILLA with conspiracy to commit computer fraud, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the defendants committed the offense alleged in the complaint.

3. The information in this affidavit is based on my personal knowledge, interviews of witnesses, my own observations and actions, information received from other law enforcement agents, my experience and training, and the experience of other agents.

FACTS ESTABLISHING PROBABLE CAUSE

Background of the Investigation

4. In or around August 2015, the FBI began investigating multiple incidents of unauthorized access of the computer systems of a healthcare services company ("Company A") with computer servers maintained by a third-party vendor ("Company B") in Franklin Park, Illinois. As explained below, between in or around October 2013 and in or around August 2015, SOLERO, VENTANILLA, and others known and unknown, accessed the computer servers of Company B for the purpose of fraudulently obtaining goods and services using promotional "points" awarded to physicians who participated in various opinion surveys conducted by Company A. In total, over 75 fraudulent reward point redemption transactions were completed using the email accounts jrsolero20@gmail.com (the "Solero Account") and yuriventanilla@gmail.com (the "Ventanilla Account") (collectively, the "Subject Accounts"), resulting in losses to Company A of at least $50,000.

5. In September 2015, FBI agents interviewed Individual A, a representative of Company A, concerning the unauthorized access and fraudulent transactions involving the Subject Accounts. Among other things, Individual A provided the following information:

a. Company A provides healthcare data science and information technology services to the healthcare industry. These services include providing physicians with opinion surveys covering multiple healthcare topics.

b. As an incentive for physicians to complete and submit the surveys it administers, Company A uses a rewards program through which physicians can earn points that can later be redeemed for various goods and services, including gift cards, electronic gift cards, airline flights, hotel vouchers, and electronic devices.

c. Company A employs Company B, a third-party marketing company with computer servers located in Franklin Park, Illinois, to manage the rewards program and points redemption process. As part of this process, Company B provides a web-based interface for its customers to manage their accounts, including the redemption of points for goods and services. A customer of Company A must supply Company B with a unique username and password to access the customer's account information and to redeem points.

d. If a customer of Company A elects to redeem points for a gift certificate, the customer may, depending upon the retailer, elect to receive either a physical gift card mailed to the customer, or an electronic gift certificate ("e-certificate") sent to an email address supplied by the customer.

Overview of the Conspiracy

6. During the September 2015 interview, Individual A explained that, beginning in or around October 2013, various customers of Company A reported that their accounts with Company A had been accessed without authorization by one or more unknown individuals, resulting in the redemption of points for goods and services that the customers had neither requested nor authorized.

7. On or about September 15, 2015, Individual A provided to the FBI records obtained from Company B showing transactions in which customer accounts had been accessed without authorization by SOLERO, VENTANILLA, and others known and unknown. Various details regarding each order were reflected in the records provided by Company A, including customer email addresses, the dates the orders were placed, names and addresses of legitimate account holders, the contents of the order, the cost of the orders in points, payment details, and the given name and address of the individual(s) to which the orders were shipped. In many instances, the address of the account holder and the address to where the order was shipped were different.

8. According to the records provided by Company A, between in or around October 2013 and August 2015, SOLERO and/or VENTANILLA accessed approximately 18 separate reward accounts administered by Company B and changed the email addresses of record to either the Solero Account or the Ventanilla Account. Each of these alterations was done without the consent of the actual account owner. Within that period, SOLERO and VENTANILLA then conducted approximately 75 different transactions in which they redeemed points contained in the victim accounts for e-certificates, gift cards, air travel, and merchandise with a total value of over approximately $52,000. None of these orders was authorized by the legitimate account owner.

9. In addition, Company B provided to the FBI a consensually-recorded telephone conversation during which VENTANILLA called Company B and asked

to change the password for an account ("Victim Account 1") owned by a participating physician. During that conversation, which occurred on or about August 7, 2015, VENTANILLA, who was using telephone number (510) 331-****,[1] represented that Victim Account 1 belonged to him and stated that he had forgotten the password for the account. Upon VENTANILLA's request, Company B changed the password for Victim Account 1 after VENTANILLA provided the correct user name. Company B was later informed, however, that Victim Account 1 belonged to another participating physician who had not authorized any password changes to the account.

10. Within a month of the August 7, 2015 password change for Victim Account 1, SOLERO and VENTANILLA redeemed points from Victim Account 1, by logging onto Victim Account 1 via the internet and conducting unauthorized transactions, for items that included international air travel and merchandise gift cards. Confirmation emails for several of these transactions were sent to both the Solero Account and the Ventanilla Account.

---

[1] Based on my review of search results from Accurint (a/k/a LexisNexis), the telephone number (510) 331-**** is associated with VENTANILLA and the address 12** Chateau Drive, San Jose, CA 95120 (an address that, as explained below, was associated with an October 23, 2014 Apple MacBook order). Based on my training and experience, I know that Accurint is a search tool that allows law enforcement to query data from a number of public and non-public record sources. Although the information provided by Accurint concerning the telephone number (510) 331-**** does not specify the nature of its association with VENTANILLA, I know that the sources canvassed by Accurint include, among others, Secretary of State filings, U.S. and Canadian business finder directories, Experian Business Reports, tax liens, FAA aircraft registrations, driver's license information, and credit header information.

Specific Instances Where SOLERO and VENTANILLA Obtained Goods and Services from Victim Accounts

11. On or about November 20, 2015, a search warrant for the Subject Accounts was issued in the Northern District of Illinois by Magistrate Judge Jeffrey T. Gilbert. Law enforcement agents have received and reviewed the search warrant results from Google for the Subject Accounts. During that review, as described below, agents found evidence of multiple fraudulent transactions in which SOLERO and VENTANILLA fraudulently obtained merchandise from the accounts of Company A's customers by accessing, via the internet, the computers of Company B.

12. For example, on or about October 28, 2013, the Ventanilla Account received an email from Company B providing a product order summary for "Yuri Ventanilla." The order was for an "Apple MacBook Pro with Retina Display – 13.3' Display 8GB 256GB Flash Storage" with a price of $1,049 (denominated as 1,049 points). Also included in the confirmation email was a pick-up location at Best Buy, 17** Harrison Street, San Francisco, CA 94103. This order information matches information provided by Company A, which shows an order processed on or about October 27, 2013 for "Yuri Douglas Ventanilla" at the home address 15*** Bayberry Lane, San Lorenzo, CA 94580.[2] In addition, the Company A information reflects

[2] This address is associated with VENTANILLA. More specifically, on or about January 5, 2015, an email was sent from the Ventanilla Account to an email address associated with an educational institution. The subject line of the email was "ID." Contained within the body of the email was an electronic scan of the front and back of a State of California driver's license in the name of "Yuri Douglas Ventanilla." Information contained on the driver's license included Ventanilla's address of "15*** Bayberry Ln., San Lorenzo, CA 94580," the same residential address provided in connection with the October 2, 2014

1,049 "Total Points Redeemed" for an "Apple MacBook Pro with Retina Display 13.3" Display, 8GB Memory, 256GB Flash Storage."

13. On or about October 23, 2014, the Ventanilla Account received an email from donotreply@bridge2solutions.net[3] providing a product order summary for "Yuri Ventanilla." This order was for an "Apple - MacBook Air (Latest Model) – 13.3' Display – Intel Core i5 - 4GB Memory - 128GB Flash Storage" with a price of 686 points. Also included was a pick-up location at "Best Buy, 31*** Courthouse Dr., Union City, CA 94587." This order information matches information provided by Company A showing an order processed on or about October 23, 2014 for "Yuri Douglas Ventanilla" at the address "12** Chateau Drive, San Jose, CA 95120." In addition, the Company A information also shows 686 "Total Points Redeemed" for an "Apple MacBook Air (Latest Model), 13.3" Display, Intel Core i5, 4GB Memory, 128GB Flash Storage."

14. From October 13, 2014 to December 11, 2014, the Ventanilla Account received approximately 17 emails from "donotreply@bridge2solutions.net" related to orders made in the name of "Yuri Ventanilla." These emails were for the purpose of confirming reward point transactions for items including electric appliances, personal electronics, and software. For each of these orders, the order information provided by Company A matches the order information sent to the Ventanilla Account.

Sofitel Philippine Plaza order. Also included on the driver's license was Ventanilla's date of birth and his photograph.

[3] According to Individual A, the email address "donotreply@bridge2solutions.net" is used by Company B to send confirmations for reward point transactions.

15. Emails obtained following execution of the November 20, 2015 search warrant also show that SOLERO and VENTANILLA conspired to redeem award points from Company A for travel services. For example, an email forwarded to the Solero Account from the Ventanilla Account on or about October 21, 2014, reflects an airline travel reservation for "Yuri Douglas Ventanilla" from San Francisco, California to Manila, Philippines between November 2, 2014 and November 7, 2014. Within the email was the phrase, "I CAN'T WAIT MY LOVE." In addition, the original email, which was from Philippine Airlines and was sent to the Ventanilla Account, contained an electronic copy of the airline travel order receipt. That receipt reflected an airline travel reservation for "Yuri Douglas Ventanilla" with an issue date of October 17, 2014. This information matched information provided by Company A showing an order processed on or about October 17, 2014 in the name "Yuri Douglas Ventanilla" at the home address 15*** Bayberry Lane, San Lorenzo, CA 94580. In addition, records from Company A reflect that the order was for air transportation between San Francisco, California and Manila, the Philippines. According to Company A, the points redeemed for this travel were drawn without authorization from an account belonging to a Company A customer in Englewood, New Jersey.

16. In addition, an email with the subject line "PPMIMS Order" that was forwarded from the Ventanilla Account to the Solero Account on or about October 23, 2014 also shows the redemption of rewards points for travel. More specifically, the email reflects a hotel reservation summary for "John Reynald Solero" at the

Peninsula Manila hotel in the Philippines from November 3, 2014 to November 8, 2014. This order information matches order information provided to the FBI by Company A detailing an order processed on or about October 17, 2014 in the name "John Reynald Solero" at the home address 15*** Bayberry Lane, San Lorenzo, CA 94580. In addition, the Company A information shows that the order was for the "Peninsula Manila." According to Company A, the points redeemed for this travel were drawn without authorization from an account belonging to a Company A customer.

17. On or about July 26, 2015, the Solero Account received an email from Company B providing a flight reservation summary for a trip on Emirates Airlines between August 28, 2015 and September 7, 2015. According to the email, the reservation was in the name of "John Reynald Solero" and reflected travel between Manila, the Philippines and Dubai, United Arab Emirates; Dubai to Amsterdam, Netherlands; Amsterdam back to Dubai; and Dubai back to Manila. This order information is consistent with order information provided by Company A. According to Company A, the points redeemed for this travel were drawn without authorization from an account belonging to a Company A customer in Denver, Colorado.

18. On or about July 29, 2015, the Solero Account received an email from Company B providing a hotel reservation summary for "Yuri Ventanilla" at the Hyatt Paris Madeline Hotel in Paris, France on September 4-6, 2015. This order information is consistent with order information provided by Company A. According

to Company A, the points redeemed for this travel were drawn without authorization from an account belonging to a Company A customer in Long Beach, California.

19. Also on or about July 29, 2015, the Solero Account sent an email to a different email account bearing the name "johnreynald.solero@*********.com" with the subject line "Confi." Within the body of the email was a screen shot of a separate email bearing the phrase, "Your RX Panels Awards & Studies Center UserID and Password" along with an account number following Company A's name. Included in the screen shot was the message, "Dear Dr. [redacted], This e-mail is to confirm your UserID and Password to your IMS Health Awards account." Depicted farther down on the screen shot was the email address and password for the customer's account with Company A. According to Company A, the information contained in the email screen shot was sent to the Solero Account without authorization.

20. Also on or about July 29, 2015, the Solero Account received an email from Company B providing another hotel reservation summary for "John Reynald Solero" at the Renaissance Paris Hotel in Paris, France on September 1-4, 2015 2015. This order information is consistent with order information provided by Company A. According to Company A, the points redeemed for this travel were drawn without authorization from an account belonging to a Company A customer in Denver, Colorado.

21. On or about August 8, 2015, the Solero Account received an email from Company B providing a flight reservation summary for a September 6, 2015 trip on

Aer Lingus Airlines. According to the email, the reservation was in the name of "Yuri Douglas Ventanilla" and reflected travel between Paris, France and Dublin, Ireland; and Dublin to San Francisco, California. This order information is consistent with order information provided by Company A. According to Company A, the points redeemed for this travel were drawn without authorization from Victim Account 1 in Tallahassee, Florida.

22. Also on or about August 8, 2015, the Solero Account received an email from Company B providing a flight reservation summary for a trip on KLM Royal Dutch Airlines between August 28 and August 29, 2015. According to the email, the reservation was in the name of "Yuri Douglas Ventanilla" and reflected travel between San Francisco, California and Atlanta, Georgia; and Atlanta to Amsterdam, the Netherlands. This order information is consistent with order information provided by Company A. According to Company A, the points redeemed for this travel were drawn without authorization from Victim Account 1 in Tallahassee, Florida.

Additional Information Concerning Unauthorized Access of Accounts Belonging to Customers of Company A

23. On or about August 4, 2015, the Solero Account sent an email to johnreynald.solero@*********.com with the subject line "cells" and four attachments that included the following information:

a. A spreadsheet containing the "Doctor Number," "First Name," "Last Name," "User ID," and "Points" for 207 customers of Company A;

b. A second spreadsheet containing the same categories of information for 382 additional customers of Company A;

c. A third spreadsheet containing the same categories of information for 111 additional customers of Company A; and

d. A fourth spreadsheet containing the same categories of information for 204 additional customers of Company A.

24. Based on my training and experience, as well as my knowledge of this investigation, I believe that the email described above details defendants' unauthorized access and use of hundreds of accounts belonging to customers of Company A for the purpose of furthering their scheme to defraud Company A.

Additional Evidence Relating to Defendants' Ownership of the Subject Accounts

25. On or about September 2, 2015, Google provided to the FBI subscriber and login history records for the Ventanilla Account. According to these records, the Ventanilla Account was subscribed to "Yuri Douglas Ventanilla" with an associated telephone number of (510) 331-****, the same telephone number that, as described

above, is associated with VENTANILLA and that was used on or about August 7, 2015 to change the associated email for Victim Account 1 without authorization.

26. Google also provided to the FBI subscriber and login history records for the Solero Account. According to these records, the Solero Account was subscribed to "JR Solero" with an associated telephone number located in the Philippines. In addition, based on agents' review of a database of assigned internet protocol addresses, the IP address used to set up the account belonged at that time to an internet service provider located in the Philippines.

27. Based on information provided by Company A, an individual named "John Reynald Solero" was employed by Company A in the Philippines until in or around February 2014. According to Company A, John Reynald Solero provided a resume in connection with his employment; Company A has since provided that resume to the FBI. Based on a review of the resume, agents determined that the Solero Account is listed as the email address for John Reynald Solero under a heading entitled "Contact Details." In addition, other documents provided to the FBI by Company A include a Republic of the Philippines National Bureau of Investigation clearance document that, according to Company A, Solero provided to Company A in connection with his employment at Company A. Based on agents' review, the clearance document contains SOLERO's name, address, birth date, and photograph.[4]

---

[4] Moreover, in a transaction completed on or about October 2, 2014 for travel services under the name "John Reynald Solero," SOLERO and VENTANILLA provided Company B with the address 15*** Bayberry Lane, San Lorenzo, CA 94580. As described above, the 15*** Bayberry address is associated with VENTANILLA.

28. In a transaction completed on or about October 2, 2014, SOLERO and VENTANILLA redeemed points from a victim account for the purpose of obtaining a reservation at the Sofitel Philippine Plaza Manila hotel in the Philippines. For this transaction, SOLERO and/or VENTANILLA provided Company B with the name "John Reynald Solero," along with the address 15*** Bayberry Lane, San Lorenzo, CA 94580.

29. On or about September 4, 2015, SOLERO sent an email from the Solero Account to multiple email addresses containing pictures of SOLERO in front of what appear to be the Eiffel Tower and other Paris landmarks. Included in the body of the email is the following message: "Hi Friends, Sorry for the late update. Sobrang ganada ditto sa Europe. Miss you guys." According to an open-source computer translation, the sentence "Sobrang ganada ditto sa Europe" is in the Tagalog language (a principal language of the Philippines) and means "Super nice here in Europe." Moreover, based on my review of the photograph that, as described above, SOLERO provided to Company A in connection with his employment, the individual in the Company A photograph and the individual in the September 4, 2015 Paris photographs are very similar in appearance.

CONCLUSION

30. Based upon the foregoing, I respectfully submit that there is probable cause to believe that, from in or around October 2013 to in or around August 2015, John Reynald SOLERO and Yuri VENTANILLA conspired with each other and with others known and unknown, knowingly and with intent to defraud, to access a protected computer, without authorization, in violation of 18 U.S.C. §§ 1030(b) and 1040(a)(4).

FURTHER AFFIANT SAYETH NOT.

ROBERT MEININGER
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me on March 4, 2016.

SHEILA FINNEGAN
United States Magistrate Judge